STATEWIDE

STANDARD

State of Arizona

STATEWIDE STANDARD (8350): SYSTEM AND COMMUNICATION PROTECTION

DOCUMENT NUMBER:	S8350
EFFECTIVE DATE:	April 5, 2024
REV:	1.1

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-4254 and § 41-4282.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

3. SCOPE

3.1 **Application to Budget Units (BU)** - This standard shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 **Application to Systems** - This standard shall apply to all state information systems. Standard statements preceded by “(P)” shall be required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

3.3 **Federal Government Information** - Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1. PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1. Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2. IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider statewide information security PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.2. BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	**Exception**	**Rationale**

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

a. Be ultimately responsible for the correct and thorough completion of information security PSPs throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the Director the risk to state systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC) shall:

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of Agency information security PSPs within the BU;

b. Ensure BU compliance with System and Communication Protections Policy; and

c. Promote efforts within the BU to establish and maintain effective use of agency systems and assets.

5.5 BU Chief Information Officer (CIO) shall:

a. Work with the BU Director to ensure the correct and thorough completion of Agency information security PSPs within the BU; and

b. Ensure System and Communication Protections Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU ISO shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU information security PSPs;

b. Ensure the development and implementation of adequate controls enforcing the System and Communication Protections Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the protection of agency systems and their communications.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on System and Communication Protections Policies; and

b. Monitor employee activities to ensure compliance.

5.8 System Users of agency systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding the establishment and maintenance of user accounts for agency systems.

6. STATEWIDE POLICY

6.1 **(P) Implement DMZ** – The BU shall ensure the state information system prohibits direct public access between the Internet and any system component in the Protected state information system. The DMZ shall: [PCI DSS 1.3]

a. Limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [PCI DSS 1.3.1]

b. Limits inbound Internet traffic to IP addresses within the DMZ; [PCI DSS 1.3.2]

c. Does not allow any direct connections inbound or outbound for traffic between the Internet and the Protected state information system; [PCI DSS 1.3.3]

d. Does not allow internal addresses to pass from the Internet into the DMZ; [PCI DSS 1.3.4]

e. Does not allow unauthorized outbound traffic from the Protected state information system to the Internet; [PCI DSS 1.3.5]

f. Implements stateful inspection, also known as dynamic packet filtering (i.e., only established connections are allowed into the network); [PCI DSS 1.3.6]

g. Places system components that store Confidential data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks; and [PCI DSS 1.3.7]

h. Does not disclose private IP addresses and routing information to unauthorized parties (Note: methods to obscure IP addressing may include: NAT, placing servers behind proxy servers, removal route advertisements for private networks that employ registered addressing, or internal use of RFC 1918 address space instead of registered addresses). [PCI DSS 1.3.8]

6.2 **(P) Firewall Configuration** – The BU shall build firewall and router configurations that restrict connections between Non-Protected systems (Standard state information systems or untrusted networks) and any system components in the Protected state information system. The configurations shall: [PCI DSS 1.2]

a. Restrict inbound and outbound traffic to that which is necessary for the Protected state information system; [PCI DSS 1.2.1]

b. Secure and synchronize router configuration files; and [PCI DSS 1.2.2]

c. Implement perimeter firewalls between any wireless networks and the Protected state information system, and these firewalls are configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Protected state information system. [PCI DSS 1.2.3]

6.3 Acceptable Encryption Algorithms – The following encryption algorithms are considered acceptable for use in state information systems to protect the transmission or storage of Confidential information and Protected system access.

a. (P) Acceptable Security Strength – the security strength of an encryption algorithm is a projection of the time frame during which the algorithm and the key length can be expected to provide adequate security. The security strength of encryption algorithms is measured in bits, a measure of the difficulty of discovering the key.

- The current minimum key strength for Protected state information systems and Confidential data is 112 bits.

b. Symmetric Encryption Algorithms – The following symmetric encryption algorithms are considered acceptable for use in state information systems:

Algorithm	Acceptable Key Strengths	References
Advanced Encryption Standard (AES)	• 128 bits • 192bits • 256 bits	FIPS 197
Triple Data Encryption Algorithm (TDEA) (three key 3DES)	• 168 bits	NIST SP 800-67

c. Key Agreement Schemes – The following key agreement schemes are considered acceptable for use in state information systems.

Key Agreement Scheme	Acceptable Key Strengths	References
Diffie-Hellman (DH) or MQV using Finite Fields	• P = 2048 • Q = 224 or 256	NIST SP 800-56A NIST SP 800-135

Diffie-Hellman (DH) or MQV using Elliptical Curves	• N: 224-255 and H=14 • N: 256-383 and H=16 • N: 384-511 and H=24 • N: 512+ and H=32	NIST SP 800-56A NIST SP 800-135
RSA-based	• N = 2048+	NIST SP 800-131A

d. **Hash Functions** – The following hash functions are considered acceptable for use in state information systems.

Digital Signature Generation	Digital Signature Verification	Non-digital Signature Generation Applications
• SHA-224 • SHA-256 • SHA-384 • SHA-512	• SHA-224 • SHA-256 • SHA-384 • SHA-512	• SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512

e. **Digital Signature Algorithms** – The following digital signature algorithms are considered acceptable for use in state information systems.

Digital Signature Algorithm	FIPS Publication	Digital Signature Generation Settings	Digital Signature Verification Settings	Relative Strength
Digital Signature Standard (DSA)	FIPS 186-4	p >= 2048, q = 224	p >= 2048, q = 224	>= 112 bits
RSA Digital Signature	FIPS 186-4	2048	2048	>= 112 bits
ECDSA	FIPS 186-4	224	224	>= 112 bits

f. **Message Authentication Codes** – The following message authentication codes are considered acceptable for use in state information systems.

Hash Algorithms	Hash Generation	Hash Verification
HMAC	>=112 bits	>=112 bits
CMAC	AES, 3DES	AES, 3DES
CCM and GCM/GMAC	AES	AES

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), NIST Special Publication 800-56A, April 2018

8.2 Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised), NIST Special Publication 800-67, November 2017

8.3 Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms
and Key Lengths, NIST Special Publication 800-131A, March 2019.

8.4 Recommendations for Existing Application-Specific Key Derivation Functions, Revision 1, NIST Special Publication 800-135, December 2011

8.5 Digital Signature Standard (DSS), Federal Information Processing Standards Publication, FIPS PUB 186-4, February 3, 2023

8.6 Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, FIPS PUB 197, May 9, 2023

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	**Initial Release**	**1.0**	**Aaron Sandeen, State CIO and Deputy Director**
04/05/2024	**Review**	**1.1**	Ryan Murray (Apr 5, 2024 09:31 PDT) **Ryan Murray, Deputy Director of Arizona Department of Homeland Security & Interim State Chief Information Security Officer**